Heuristic Behavior Pattern Matching of Data Flows in
Enhanced Network Traffic Classification

Abstract of the Disclosure

[0096] Methods, apparatuses and systems facilitating enhanced classification of network traffic. As discussed above, typical mechanisms that classify network traffic analyze explicitly presented or readily discoverable attributes of individual packets against an application signature, such as a combination of protocol identifiers, port numbers and text strings. The present invention extends beyond analysis of such explicitly presented packet attributes and holistically analyzes data flows, and in some implementations, related data flows against known application behavior patterns to classify the data flows. Implementations of the present invention facilitate the classification of encrypted or compressed network traffic, or where the higher layer information in the data flows are formatted according to a non-public or proprietary protocol. In one embodiment, the enhanced classification functionality analyzes the behavioral attributes of encrypted data flows against a knowledge base of known application behavior patterns to classify the data flows. In one embodiment, the enhanced classification mechanisms described herein operate seamlessly with other Layer 7 traffic classification mechanisms that operate on attributes of the packets themselves. Implementations of the present invention can be incorporated into a variety of network devices, such as traffic monitoring devices, packet capture devices, firewalls, and bandwidth management devices.